DOI: https://doi.org/10.52756/ijerr.2024.v46.016 *Int. J. Exp. Res. Rev.*, Vol. 46: 202-211 (2024)

Original Article | *Peer Reviewed* | *Open Access*

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in
ISSN 2455-4855

Mapping the Cybersecurity Research: A Comprehensive Bibliometric Analysis

Poonam Khurana[1], Swati Narula[2], Neelu Tiwari[3], Renuka Kapoor[4]* and Madhu Arora[5]

[1]Vivekananda Institute of Professional Studies, VIPS-TC, GGSIPU, Delhi, India; [2]Vivekananda School of Business Studies, VIPS-TC, GGSIPU, Delhi, India; [3]Jaipuria Institute of Management, Delhi, India; [4]Amity School of Business, Amity University, Noida, India; [5] New Delhi Institute of Management, Delhi, India

E-mail/Orcid Id:

PK, dr.poonamkhurana05@gmail.com, https://orcid.org/0000-0001-5134-9147; *SN,* swati.narula@vips.edu, https://orcid.org/0009-0009-5497-5739; *NT,* neelutiwari82@gmail.com, https://orcid.org/0000-0002-6733-3665; *RK,* kapoorrenuka.123@gmail.com, https://orcid.org/0009-0006-8138-4625; *MA,* aroramadhu86@gmail.com, https://orcid.org/0000-0002-9554-3176

Article History:

Received: 04th Aug., 2024
Accepted: 20th Dec., 2024
Published: 30th Dec., 2024

Keywords:
Artificial intelligence, Bibliometric analysis, Cyber security, Cyber threat, Privacy, Technology

How to cite this Article:
Saranya, A., Sivakumari, K., Rajesh, S., Shyamala Devi, K., Padmavathy, K., & Hemalatha, M. (2024). Evaluation of Antioxidant, Anti-inflammatory and Antimicrobial Potential of *Aegel marmelos* Fruit Pulp Extracts against Clinical Pathogens. *International Journal of Experimental Research and Review*, *46*, 202-211.
DOI:
https://doi.org/10.52756/ijerr.2024.v46.016

Abstract: The present study conducted a bibliometric analysis to synthesise available literature on cybersecurity. The analysis identifies prolific authors, relevant sources, affiliations, nations, trend topics, publication trends, themes, and collaboration patterns among countries. Scopus database was searched using the keyword "cyber security" and the search resulted in 31,852 articles. After the inclusion and exclusion criteria, a total of 733 documents were extracted in a CSV format for analysis. The Biblioshiny web tool of the R-package was used for analysis. The finding shows an exponential rise in scholarly work on cybersecurity. "Information and computer security" is identified as the most relevant source. Chen H has published most articles and the USA leads the field in terms of publication, global citations, and collaboration with other countries. The trend topics and themes have also been listed. The study would help readers understand the landscape of cybersecurity research, identify key contributors, and guide them in addressing the challenges posed by cyber threats.

Introduction

The world is experiencing a remarkable cyberspace expansion, greatly increasing access to information. However, this rapid development also provides opportunities for those with malicious intentions. As a result, it has become essential to protect systems and technologies from suspicious or harmful activities (Kaur and Ramkumar, 2022; Chetry and Sharma, 2023). Cyber security safeguards computer systems, networks, and data, preventing disruptions and unauthorized access, use, disclosure, alteration, or destruction (Thakur et al., 2016; Awasthi and Goel, 2024; Jha et al., 2024). Cyber security plays a crucial role in preventing cyber-attacks and data breaches while also assisting in managing risks. Cyber threats can approach from unexpected sources and directions. As technology advances, we are witnessing increasingly sophisticated cybercrimes and malicious activities, which are highly targeted and pose significant dangers in today's world.

During the early days of the internet, cyber threats were quite basic, usually involving individual hackers attempting to disrupt systems for entertainment or fame. However, with technological advancements, the complexity and magnitude of cyber-attacks have grown considerably. Threats such as Cyberbullying, digital devices, wireless body area networks, identity theft,

***Corresponding Author:** kapoorrenuka.123@gmail.com

wireless sensor networks, and autonomous systems are common these days ("Computer Security Handbook," 2012; Kaur and Ramkumar, 2022; Parkinson et al., 2017; Roy et al., 2019; Smit, 2015). Websites, web applications, and computer systems are susceptible to various forms of attacks, making cyberspace a fertile ground for cybercriminal activities. Due to technology's diverse and complex nature, computer systems are easily accessible and vulnerable to unauthorized access or breaches. Cybercriminals take advantage of human vulnerabilities and careless attitudes toward protecting computer systems, allowing them to gain access and control over those systems (Razzaq et al., 2013).

Li and Liu (2021) explained various types of network security for better protection. Cyber security ensures that access to information is restricted to authorized individuals only. Network security safeguards computer networks against disruptions caused by malware and hacking (Zhang, 2021). It encompasses a range of solutions that help organizations protect their networks from hackers, organized attackers, and malicious software. Application security (Alkatheiri, Chauhdary, & Alqarni, 2021) involves using hardware and software tools, such as antivirus programs, encryption, and firewalls, to safeguard the system from external threats that could disrupt application development. Information security safeguards physical and digital data from unauthorized access, disclosure, misuse, modification, and deletion (Ogbanufe, 2021). Operational security (Ogbanufe, 2021) encompasses the processes and decisions implemented to manage and safeguard data. This includes setting user permissions for network access and defining the protocols for when and where information can be stored or shared. Cloud Security (Krishnasamy & Venkatachalam, 2021) safeguards information stored in the cloud through software solutions and monitors for on-site attack risks to mitigate potential threats.

International Telecommunication Union proposed measures for cyber security and classified them into legal, technical, organisational, capacity building and corporation aspects (ITU, 2015; Jones, 1997; Maglaras et al., 2019). Legal measures are designed to establish legislation and a regulatory framework for protecting cyberspace. Several best practices are recommended: first, conducting mandatory periodic assessments of critical infrastructures through information security audits is essential. Additionally, organizations should verify that the software and hardware tools used within the critical infrastructure comply with recognized security standards. Technical measures involve the use of technological tools, both software and hardware, to prevent, detect, and respond to cyber-attacks. This includes implementing internationally recognized security standards within organizations, particularly those handling critical infrastructure. Organizations should also deploy preventive and detective security tools, such as firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). Furthermore, it is essential to establish measures for physical security, access control, regular patching and upgrades, and forensic analysis. Developing a robust incident response capability is also crucial for effectively addressing potential threats. Capacity-building measures focus on enhancing knowledge and expertise to promote cyber security. To support this, it is recommended that IT specialists in critical infrastructure sectors obtain certifications from internationally recognized cybersecurity programs. Additionally, conducting periodic awareness and training programs for employees is essential to keep them informed and prepared against potential cyber threats. Cooperation measures focus on fostering partnerships among various stakeholders to enhance organisations' cyber resilience against cyber threats. To achieve this, it is recommended that reliable information-sharing mechanisms regarding threats and vulnerabilities between private and public entities be established. Additionally, creating a cooperative framework between industry and research can help promote cyber security and bolster resilience against attacks. Building collaboration frameworks between countries on various cybersecurity aspects is also essential. Furthermore, contributing to international efforts aimed at protecting cyberspace is crucial for a collective response to cyber challenges (Maglaras et al., 2019).

The increasing prevalence and sophistication of cyber threats have made cybersecurity a critical area of research and practice. With rising digital transformation, cyber crimes are also escalating. It is essential to understand the landscape of cybersecurity research, identify key contributors, and guide addressing the challenges posed by cyber threats. The present study conducted a bibliometric analysis to provide a comprehensive analysis of the existing literature on cybersecurity. The study aims to identify key authors, annual scientific production, relevant sources and affiliations, most relevant documents, trend topics, thematic analysis and collaboration patterns among countries. The study fosters collaboration among researchers and practitioners, informing policy-making efforts in cyber security.

Research Questions

#What are the publication trends in cyber security research?

DOI: https://doi.org/10.52756/ijerr.2024.v46.016

#What are the relevant authors, sources, documents, and affiliations in cyber security research?

#What are the trend topics and themes in cybersecurity research?

#What is the collaboration pattern among countries in cyber security research?

Method

The study performed bibliometric analysis to understand influences on cyber security and how the literature on cyber security is structured. The Scopus database was chosen for extracting articles. The Scopus database was chosen since it has the largest number of high-quality scientific publications (Heradio et al., 2016). The keyword “cyber security” was searched and without any filter, the initial search returned 31,852 articles. Only final articles published in the business and management domain were included. The articles published in the journal in English were considered and excluded conference proceedings, book chapters, and press articles. After inclusion and exclusion criteria, a total of 733 documents were collected and extracted in a CSV file. The search string is given as:

“TITLE-ABS-KEY ("cyber security") AND (LIMIT-TO (DOCTYPE, "ar")) AND (LIMIT-TO (LANGUAGE, "English")) AND (LIMIT-TO (SRCTYPE, "j")) AND (LIMIT-TO (PUBSTAGE, "final")) AND (LIMIT-TO (SUBJAREA, "BUSI"))”

The PRISMA framework for sample selection is demonstrated in Figure 1.

For Analysis, the Bibliometrix R-package was employed. R-package was developed by Aria and Cuccurullo and written in the R language. It is used in scientific and statistical mapping analysis (Aria & Cuccurullo, 2017). Biblioshiny, a web-based interface, was added to conduct bibliometric analysis. The analysis is discussed in the next section

Result and Discussion

Descriptive analysis

A thorough information acquired from the Scopus database is shown in Table 1. It was found that between 2003 to 2024, 733 articles were published in 234 distinct sources. The annual growth rate of cyber security research is 21.08%, indicating that the research area is growing significantly. 1964 authors have contributed to the body of knowledge in this field, and 125 authors have been published as single authors. In cyber security research, a total of 2342 authors' keywords were used. International collaboration is 20.19%, which indicates strong cooperation on shared global issues such as cyber security.

Publication trend

Year-wise publication on cyber security from 2003 to 2024 is shown in Figure 2. Publication trends show a significant rise over the years. Very few articles were initially published, but the number has risen exponentially since 2015. The highest publication was in the year 2023. Future scholars are suggested to contribute to the body of knowledge on this rising area.

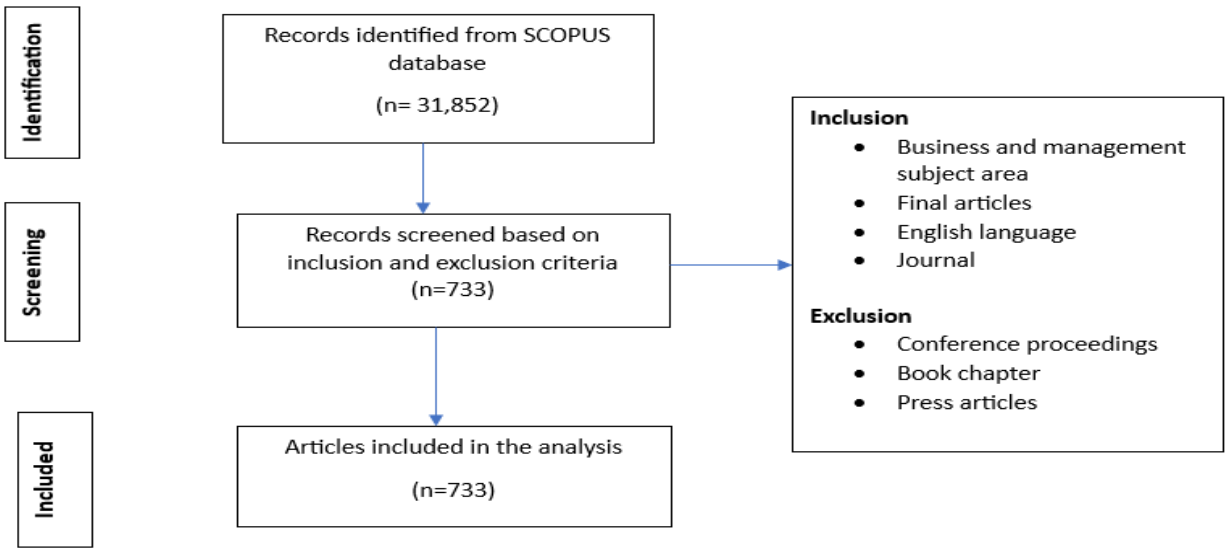

Figure 1. PRISMA framework.

Table 1. Descriptive analysis.

Main information about data	
"Timespan	2003 : 2024
Sources (Journals, Books, etc)	234
Documents	733
Annual Growth Rate %	21.08
Document Average Age	3.78
Average citations per doc	17.11
References	34037
DOCUMENT CONTENTS	
Keywords Plus (ID)	2938
Author's Keywords (DE)	2342
AUTHORS	
Authors	1964
Authors of single-authored docs	125
AUTHORS COLLABORATION	
Single-authored docs	127
Co-Authors per Doc	2.94
International co-authorships %	20.19
DOCUMENT TYPES	
article	733"

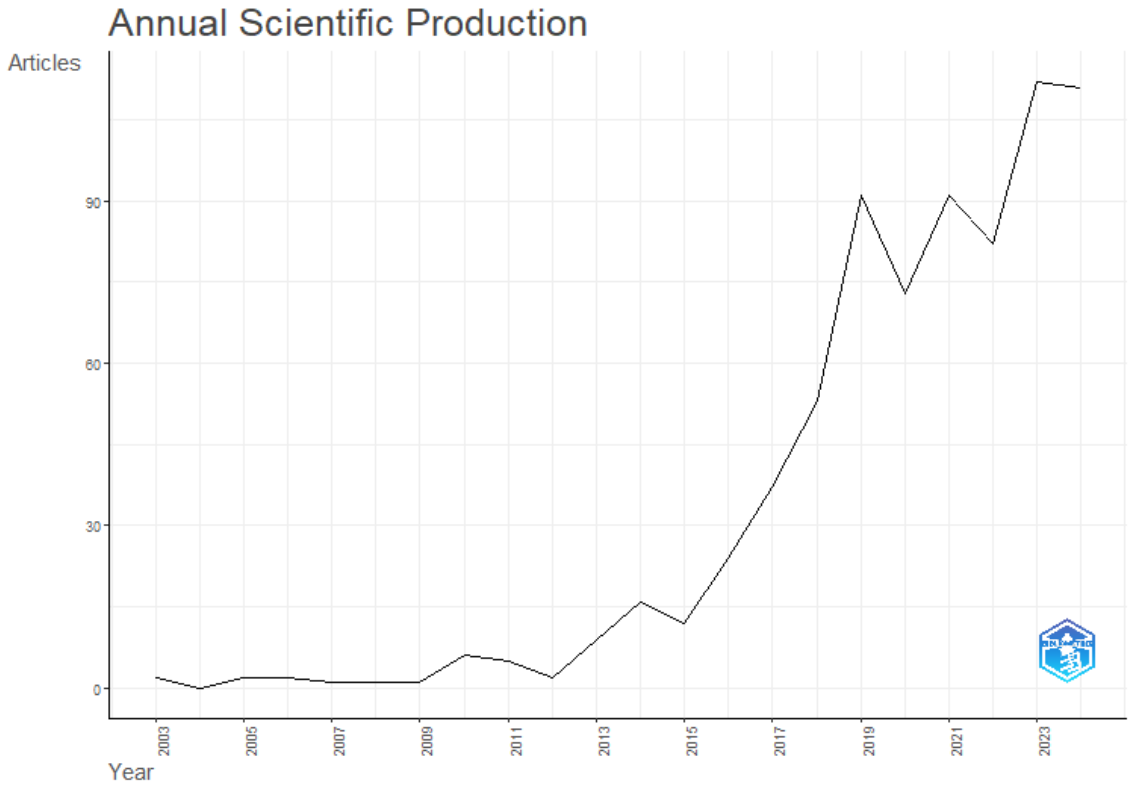

Figure 2. Publication trend.

Most Relevant Sources

Top 10 sources are listed in Table 2. Scholars can find literature on cyber security using this list. "Information and Computer Security" has published most articles (59), following "Computer Law and Security Review" (52) and "International Journal of Recent Technology and Engineering" (27). The journals listed are indexed in Scopus, ensuring quality publication.

Most Relevant Authors

A list of the top 10 Authors based on the number of articles is given in Table 3. Chen H published the most articles (8), following Renaud K (7) and Samtani S (6).

Scholars who are interested in cybersecurity research can read the publications of these top authors. Scholars can also connect with them for collaborative work.

Table 2. Most Relevant Sources.

Sources	Articles
Information and Computer Security	59
Computer Law and Security review	52
International Journal of Recent Technology and Engineering	27
IEEE Transactions on Engineering Management	22
Technology in Society	19
International Journal of Scientific and Technology Research	17
Economist (United Kingdom)	16
Big Data and Cognitive Computing	14
Decision Support Systems	13
Journal of Network and Systems Management	13

Table 3. Most Relevant Authors.

Authors	Articles
CHEN H	8
RENAUD K	7
SAMTANI S	6
LI Z	5
ZHANG Y	5
AHMAD A	4
JR	4
LI Y	4
BONGIOVANNI I	3
BROMALL N	3

Most Relevant Affiliation

The list of top 10 affiliations based on articles published is given in Table 4. "UNIVERSITY OF MELBOURNE" has most articles published (11) following "UNIVERSITY OF PORTSMOUTH" (10), "RMIT UNIVERSITY VIETNAM" (9) and "UNIVERSITY OF ARIZONA" (9).

Table 4. Most Relevant Sources.

Affiliation	Articles
University of Melbourne	11
University of Portsmouth	10
Rmit University Vietnam	9
University of Arizona	9
Defence Science and Technology Group	8
Ionian University	8
University of Campinas-Unicamp	8
University of East London	8
Bournemouth University	7
Deakin University	7

Most Global Cited Documents

Top 10 globally cited documents are listed in Table 5. The list would benefit scholars by allowing them to find the most globally cited documents on cybersecurity. The article "Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life" has received highest global citation (673) following "Blockchain's roles in strengthening cybersecurity and protecting privacy" (463) and "Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration" (370).

Trend topics

Table 6 lists the trend topics based on Authors keywords. The list would help the researcher to identify trend topics to work on. The scholars can add knowledge on the variables listed, highlighting their relevance in the current scenario. The list has top 10 keywords. Cybersecurity is the most used variable (388), followed by information security (43) and machine learning (34). Due to their relevance and low exploration, working on the least used variables, such as cyber risk, privacy, security, and blockchain would also be relevant.

Thematic analysis

Based on relevance and development degree, four themes were identified: the "motor theme, Niche theme, Emerging theme, and the basic theme" (Figure 3). The basic themes have high relevance but are less developed.

DOI: https://doi.org/10.52756/ijerr.2024.v46.016

Table 5. Most Global cited documents.

Paper	DOI	Reference	Total Citations
Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life	10.1016/j.ijinfomgt.2020.102211	Dwivedi et al., 2020	673
Blockchain's roles in strengthening cybersecurity and protecting privacy	10.1016/j.telpol.2017.09.003	Kshetri, 2017	463
Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration	10.1108/BPMJ-04-2017-0088	Ardito et al., 2019	370
The economic incentives for sharing security information	10.1287/isre.1050.0053	Gal-Or & Chose, 2005	278
Sharing information on computer systems security: An economic analysis	10.1016/j.jaccpubpol.2003.09.001	Gordon et al., 2003	237
Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance	10.25300/MISQ/2019/15117	Alec Cram et al., 2019	222
Decision support approaches for cyber security investment	10.1016/j.dss.2016.02.012	Fielder et al., 2016	195
A survey of the applications of text mining in financial domain	10.1016/j.knosys.2016.10.003	Kumar and Ravi, 2016	188
Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain	10.1080/07421222.2018.1550550	Yin et al., 2019	165
Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry	10.1016/j.jik.2021.01.002	Aslam et al., 2021	159

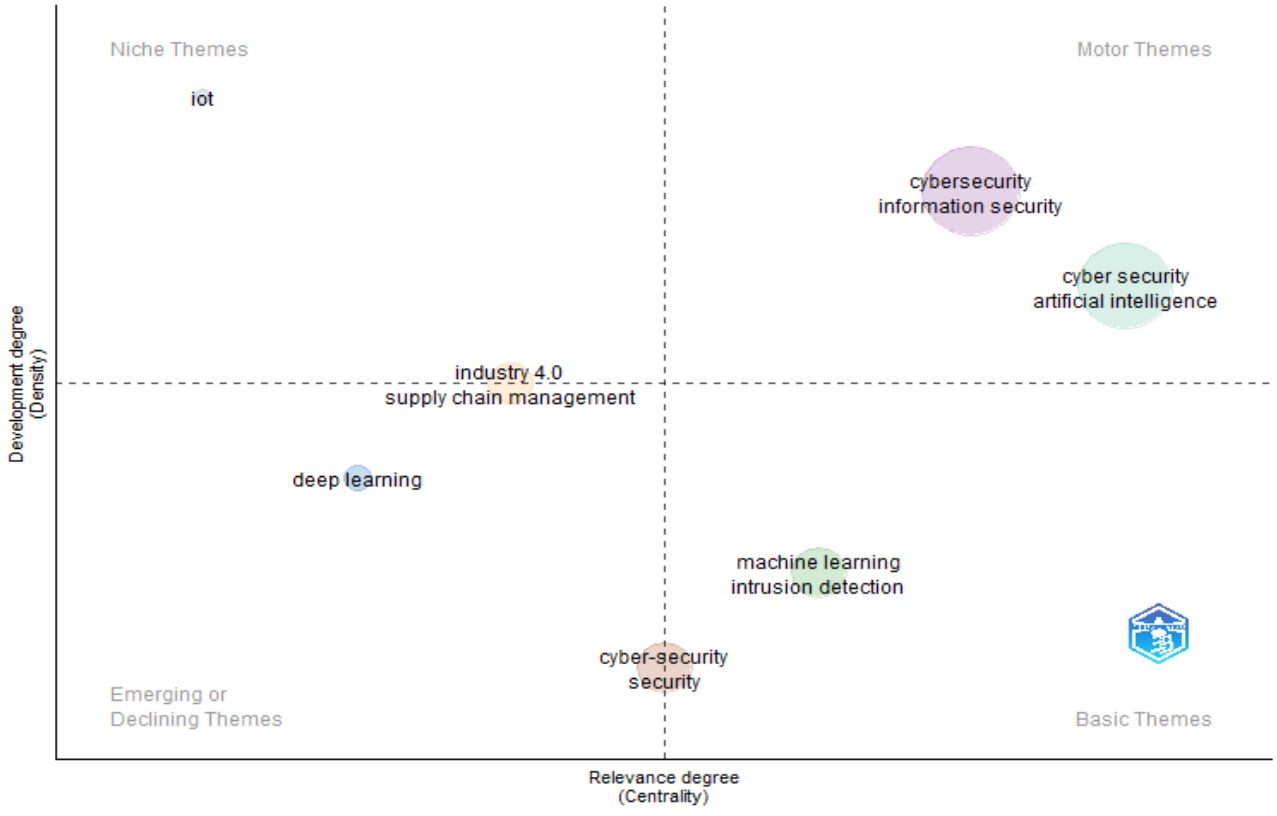

Figure 3. Thematic analysis.

Scholars are suggested to extend the literature on the basic themes (Khurana& Kapoor,2024). The identified basic themes are ("machine learning and intrusion detection") and ("security and cybersecurity). The emerging themes can emerge or decline in future, having less relevance and development. The identified emergence themes are ("deep learning"). The motor themes have high relevance and have developed so far. The motor themes are well explored and identified as ("cybersecurity and information security) and ("cybersecurity and artificial intelligence). The niche theme has less relevance and is a more developed theme. Researchers are advised not to contribute to such themes. The identified Niche themes are ("Internet of things-Iot") and ("Industry 4.0 and supply chain management").

Countries performance

Countries' scientific production, most cited countries and collaboration are listed in Tables 7,8 and 9 respectively. The USA has the most publications (431), followed by India (248) and the UK (177). It is evident from the list that India's research on cybersecurity is rising and scholars can contribute to the ongoing research on cybersecurity. The USA has also received the most global citations (2399), following the UK (1674) and Australia (656). India is also in the top 10 list, indicating global recognition of research work on cyber security by Indian scholars. Most collaboration work is done between the USA and India (8 articles), following the USA and UK (6). It is evident from the list that the USA collaborates the

Table 6. Trend Topics.

Items	Frequency
cybersecurity	388
information security	43
machine learning	34
artificial intelligence	25
Internet of things	23
cybercrime	22
blockchain	22
security	20
privacy	15
cyber risk	14

Table 7. Country Scientific Production.

Country	Frequency
USA	431
INDIA	248
UK	177
UKRAINE	133
AUSTRALIA	100
CHINA	72
MALAYSIA	58
ITALY	54
NETHERLANDS	44
CANADA	41

Table 8. Most Cited Countries.

Country	Total Citation
USA	2399
UNITED KINGDOM	1674
AUSTRALIA	656
ITALY	616
INDIA	571
SOUTH AFRICA	308
CHINA	289
GERMANY	231
NETHERLANDS	205
BELGIUM	193

DOI: https://doi.org/10.52756/ijerr.2024.v46.016

most with other countries. The graphical representation of global collaboration is shown in Figure 4.

Table 9. World collaboration.

From	To	Frequency
USA	INDIA	8
USA	UNITED KINGDOM	6
UNITED KINGDOM	CHINA	5
USA	CANADA	5
USA	CHINA	5
INDIA	UNITED KINGDOM	4
USA	AUSTRALIA	4
USA	GERMANY	3
USA	ISRAEL	3
USA	KOREA	3

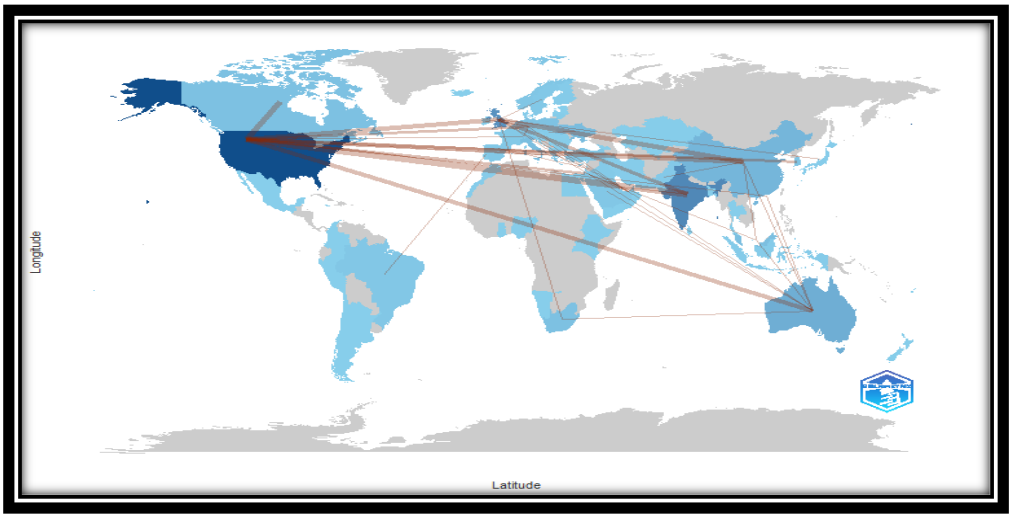

Figure 4. World Collaboration Network.

Conclusion

Cybersecurity is essential to safeguard the digital system against increasing cyber threats. Ensuring security in the digital age is about technology and fostering a culture of awareness, collaboration, and preparedness across all sectors. To ensure a secure and resilient cyberspace, continuous research and innovation are needed to stay ahead of such threats. The present study conducted a bibliometric analysis to examine the publication trend, trend topics, and themes and identify the most prolific authors, relevant sources, affiliations, countries and collaboration patterns among countries. The analysis offers direction for research to address unexplored areas such as machine learning, intrusion detection, cyber risk, privacy and blockchain. The top cited documents were listed to help researchers get relevant literature on cybersecurity. In conclusion, this bibliometric paper provides a valuable foundation for researchers, practitioners, and policymakers by outlining the current landscape of cybersecurity research and guiding future initiatives. As cyber threats become increasingly complex, sustained research, collaboration, and policy development efforts are essential for protecting digital systems and improving global cybersecurity resilience.

Limitation

The present study has several limitations. The data for bibliometric analysis was extracted solely from the Scopus database which may not provide comprehensive coverage of all relevant publications. Only English-language publications were considered that can underrepresent research from other languages. The single keyword (cybersecurity) was used while searching literature, which might have led to a skewed understanding of the research landscape. The bibliometric analysis overlooks qualitative aspects such as originality, actual impact, and relevance of the research. Despite limitations, the present study contributes to understanding research trends, identifying performance indicators, and guiding future studies.

Conflict of Interest

The authors declare no conflict of interest.

DOI: https://doi.org/10.52756/ijerr.2024.v46.016

References

Alec Cram, W., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly: Management Information Systems*, *43*(2). https://doi.org/10.25300/MISQ/2019/15117

Alkatheiri, M. S., Chauhdary, S. H., & Alqarni, M. A. (2021). Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustainable Energy Technologies and Assessments*, *45*. https://doi.org/10.1016/j.seta.2021.101219

Ardito, L., Petruzzelli, A. M., Panniello, U., & Garavelli, A. C. (2019). Towards Industry 4.0: Mapping digital technologies for supply chain management-marketing integration. *Business Process Management Journal*, *25*(2). https://doi.org/10.1108/BPMJ-04-2017-0088

Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4). https://doi.org/10.1016/j.joi.2017.08.007

Aslam, J., Saleem, A., Khan, N. T., & Kim, Y. B. (2021). Factors influencing blockchain adoption in supply chain management practices: A study based on the oil industry. *Journal of Innovation and Knowledge*, *6*(2). https://doi.org/10.1016/j.jik.2021.01.002

Awasthi, A., & Goel, N. (2024). An Approach for Efficient and Accurate Phishing Website Prediction Using Improved ML Classifier Performance for Feature Selection. *International Journal of Experimental Research and Review*, *40*(Spl Volume), 73-89. https://doi.org/10.52756/ijerr.2024.v40spl.006

Chetry, A., & Sharma, U. (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *Int. J. Exp. Res. Rev.*, *32*, 195-205. https://doi.org/10.52756/ijerr.2023.v32.017

Computer Security Handbook. (2012). In *Computer Security Handbook*. https://doi.org/10.1002/9781118851678

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., … Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*. https://doi.org/10.1016/j.dss.2016.02.012

Gal-Or, E., & Chose, A. (2005). The economic incentives for sharing security information. *Information Systems Research*, *16*(2). https://doi.org/10.1287/isre.1050.0053

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6). https://doi.org/10.1016/j.jaccpubpol.2003.09.001

Heradio, R., De La Torre, L., Galan, D., Cabrerizo, F. J., Herrera-Viedma, E., & Dormido, S. (2016). Virtual and remote labs in education: A bibliometric analysis. *Computers and Education*, *98*. https://doi.org/10.1016/j.compedu.2016.03.010

ITU. (2015). Global Cybersecurity Index & Cyberwellness Profiles. In *4. Lain-Lain*.

Jha, K., Jain, A., & Srivastava, S. (2024). A Secure Biometric-Based User Authentication Scheme for Cyber-Physical Systems in Healthcare. *International Journal of Experimental Research and Review, 39*(Spl Volume), 154-169. https://doi.org/10.52756/ijerr.2024.v39spl.012

Jones, R. W. (1997). International Telecommunication Union. *IEEE Antennas and Propagation Society, AP-S International Symposium (Digest)*, *2*. https://doi.org/10.1386/jdtv.1.3.367_7

Kaur, J., & Ramkumar, K. R. (2022). The recent trends in cyber security: A review. *Journal of King Saud University - Computer and Information Sciences*, Vol. 34. https://doi.org/10.1016/j.jksuci.2021.01.018

Krishnasamy, V., & Venkatachalam, S. (2021). An efficient data flow material model based cloud authentication data security and reduce a cloud storage cost using Index-level Boundary Pattern Convergent Encryption algorithm. *Materials Today: Proceedings*, *81*(2). https://doi.org/10.1016/j.matpr.2021.04.303

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10). https://doi.org/10.1016/j.telpol.2017.09.003

Kumar, B. S., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems*, *114*. https://doi.org/10.1016/j.knosys.2016.10.003

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends

and recent developments. *Energy Reports*, *7*. https://doi.org/10.1016/j.egyr.2021.08.126

Maglaras, L., Ferrag, M. A., Derhab, A., Mukherjee, M., & Janicke, H. (2019). Cyber Security: From Regulations and Policies to Practice. *Springer Proceedings in Business and Economics*. https://doi.org/10.1007/978-3-030-12453-3_88

Ogbanufe, O. (2021). Enhancing End-User Roles in Information Security: Exploring the Setting, Situation, and Identity. *Computers and Security*, *108*. https://doi.org/10.1016/j.cose.2021.102340

Parkinson, S., Ward, P., Wilson, K., & Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. *IEEE Transactions on Intelligent Transportation Systems*, *18*(11). https://doi.org/10.1109/TITS.2017.2665968

Razzaq, A., Hur, A., Ahmad, H. F., & Masood, M. (2013). Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. *Proceedings - 2013 11th International Symposium on Autonomous Decentralized Systems, ISADS 2013*. https://doi.org/10.1109/ISADS.2013.6513420

Roy, M., Chowdhury, C., & Aslam, N. (2019). Security and privacy issues in wireless sensor and body area networks. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*. https://doi.org/10.1007/978-3-030-22277-2_7

Smit, D. M. (2015). Cyberbullying in South African and American schools: A legal comparative study. *South African Journal of Education*, *35*(2). https://doi.org/10.15700/saje.v35n2a1076

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2016). An Investigation on Cyber Security Threats and Security Models. *Proceedings - 2nd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2015 - IEEE International Symposium of Smart Cloud, IEEE SSC 2015*. https://doi.org/10.1109/CSCloud.2015.71

Yin, H. H. S., Langenheldt, K., Harlev, M., Mukkamala, R. R., & Vatrapu, R. (2019). Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain. *Journal of Management Information Systems*, *36*(1). https://doi.org/10.1080/07421222.2018.1550550

Zhang, J. (2021). Distributed network security framework of energy internet based on internet of things. *Sustainable Energy Technologies and Assessments*, *44*. https://doi.org/10.1016/j.seta.2021.101051

How to cite this Article:

Saranya, A., Sivakumari, K., Rajesh, S., Shyamala Devi, K., Padmavathy, K., & Hemalatha, M. (2024). Evaluation of Antioxidant, Anti-inflammatory and Antimicrobial Potential of *Aegel marmelos* Fruit Pulp Extracts against Clinical Pathogens. *International Journal of Experimental Research and Review*, *46*, 202-211.

DOI : https://doi.org/10.52756/ijerr.2024.v46.016